1437

PTO/SB/95 (08-00)
Approved for use through 05/31/2002. OMB 0651-0030
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE


# Disclosure Document Deposit Request

Mail to:

Box DD
Assistant Commissioner for Patents
Washington, DC 20231

Inventor(s): John Bartas

Title of Invention: All-In-One Network Content Filter

Enclosed is a disclosure of the above-titled invention consisting of 18 sheets of description and 0 sheets of drawings. A check or money order in the amount of 10.00 is enclosed to cover the fee (37 CFR 1.21(c)).

The undersigned, being a named inventor of the disclosed invention, requests that the enclosed papers be accepted under the Disclosure Document Program, and that they be preserved for a period of two years.

Signature of Inventor

John Bartas

Typed of printed name

1/17/03

Date

10230 Lebanon Drive

Address

Cupertino, CA 95014

City, State, Zip

## NOTICE OF INVENTORS

It should be clearly understood that a Disclosure Document is not a patent application, nor will its receipt date in any way become the effective filing date of a later filed patent application. A Disclosure Document may be relied upon only as evidence of conception of an invention and a patent application should be diligently filed if patent protection is desired.

Your Disclosure Document will be retained for two years after the date it was received by Office (USPTO) and will be destroyed thereafter unless it is referred to in a related patent a The Disclosure Document may be referred to by way of a letter of transmittal in a new pater a pending application. Unless it is desired to have the USPTO retain the Disclosure Docu required that it be referred to in the patent application.

The two-year retention period should not be considered to be a "grace period" during whic application without possible loss of benefits. It must be recognized that in establishing pri referring to a Disclosure Document must usually also establish diligence in completing the since the filing of the Disclosure Document.

DISCLOSURE DOCUMENT NO.

524711

RETAINED FOR 2 YEARS

THIS IS NOT A PATENT APPLICATION

PTO-1652 (8/99)

If you are not familiar with what is considered to be "diligence in completing the invention" or "reduction to practice" under the patent law or if you have other questions about patent matters, you are advised to consult with an attorney or agent registered to practice before the USPTO. The publication, *Attorneys and Agents Registered to Practice Before the United States Patent and Trademark Office*, is available from the **Superintendent of Documents, Washington, DC 20402.** Patent attorneys and agents are also listed in the telephone directory of most major cities. Also, many large cities have associations of patent attorneys which may be consulted.

**You are also reminded that any public use or sale in the United States or publication of your invention anywhere in the world more than one year prior to the filing of a patent application on that invention will prohibit the granting of a patent on it.**

Disclosures of inventions which have been understood and witnessed by persons and/or notarized are other examples of evidence which may also be used to establish priority.



There is a nationwide network of Patent and Trademark Depository Libraries (PTDLs), which have collections of patents and patent-related reference materials available to the public, including automated access to USPTO databases. Publications such as *General Information Concerning Patents* are available at the PTDLs, as well as the USPTO's Web site at www.uspto.gov. To find out the location of the PTDL closest to you, please consult the complete listing of all PTDLs that appears on the USPTO's Web site or in every issue of the Official Gazette, or call the USPTO's General Information Services at 800-PTO-9199 (800-786-9199) or 703-308-HELP (703-308-4357). To insure assistance from a PTDL staff member, you may wish to contact a PTDL prior to visiting to learn about its collections, services, and hours.

# DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

ATTORNEY DOCKET NO. **P1437**

---

As a below named inventor, I hereby declare that: My residence, post office address and citizenship are as stated be low next to my name. I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: **Methods and Apparatus for Monitoring Local Network Traffic on Local Network Segments and Resolving Detected Security and Network Management Problems Occurring on those Segments**

the specification of which (check one) ☒ is attached hereto.
☐ was filed on: _____ as patent application serial number
☐ and was amended on
(If applicable)

I hereby state that I have reviewed and understood the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations sec. 1.56. In the case that the present application is a continuation-in-part application, I further acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations sec. 1.56. which became available between the filing date of the prior application and the filing date of the present application. I hereby claim foreign priority benefits under Title 35, United States Code s119 of any foreign applications for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

| (Number) | (Country) | (Day/Month/Year Filed) |
|---|---|---|
| (Number) | (Country) | (Day/Month/Year Filed) |

I hereby claim the benefit under Title 35, United States Codes, sec. 119 and sec. 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, sec. 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, sec. 156(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application.

(Application Serial No.):____ (Filing Date):____ (Status):_____
(Application Serial No.):____ (Filing Date):____ (Status):_____
(Application Serial No.):____ (Filing Date):____ (Status):_____
(Application Serial No.):____ (Filing Date):____ (Status):_____
(Application Serial No.):____ (Filing Date):____ (Status):_____

POWER OF ATTORNEY: As a named inventor, I hereby appoint:

☒ Practitioners at customer number: 24739

OR

☐ Practitioners: Name: Registration number

to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Please send all correspondence practitioners at:

☒ The practitioners at the customer number indicated above

☐ Customer number: *Place customer bar code label here*

**DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION**

ATTORNEY DOCKET NO. **P1437**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or first inventor: John Alexander Dayas

1st inventor's signature: _____ Dated: 9/17/03

Residence: 10203 Lebanon Drive, Cupertino, CA 95014

Citizenship: US

Post Office Address: Same

Business Summary
January 1, 2003

COPY

## Our mission

We will be the first provider of a one-stop solution to Internet problems and network management. Our product and services will allow Internet users to reclaim their networks and stand-alone computers from Hackers, spammers, pornographers, viruses, and careless or malicious users.

## The Problem

As the Internet has grown in recent years, management problems have arisen that threaten its usefulness and even it's very existence. Hacker attacks, intrusive mass marketing, offensive content, spyware, and theft of data by malicious or careless insiders undermine the Internet's utility to every user and to society as a whole. There are over 100 Million homes and small businesses attached to the Internet today, most with high levels of frustration with these problems and no effective tools to combat them.

The tools that currently exist today are all:

- Complex – Too difficult to install and configure.
- Expensive – Most cost too much for the mass market.
- Crippling – They slow down network performance
- Incomplete – They do not solve the whole problem.

Despite these drawbacks, network security spending in the US and Canada is projected to grow from $3.8 billion in 2002 to $9.5 billion in 2006[1]. Our projected share of this market is about 19%, or $1.9 Billion, $1.7 Billion of which is profit.

## The Buster Concept

The Buster technology is a different approach to network management. Traditional solutions (firewalls, anti-virus software, web site blockers) need to be installed on every computer on the network or on the critical path between the local network and the Internet. This is cumbersome, performance robbing, and expensive.

By contrast, Buster technology works as a separate standalone module, which can be installed anywhere on the network. It monitors network traffic for

---

[1] "User plans for Security Products and services, US/Canada 2002" - Infonetics; Oct 29, 2002

problems, and only acts when trouble is detected. It can be implemented as an inexpensive box, or as a chipset added to another device such as a hub or Ethernet adapter. One Buster unit, installed anywhere on the net, can monitor the whole network segment. Since it only acts when trouble us detected, it does not degrade network performance; and even improves it by eliminating bandwidth-robbing spam, advertisements and popups.



As the network grows (as successful networks usually do) and adds more segments, busters can be added incrementally. Buster's distributed design allows it to scale linearly as networks expand. A small company which becomes large never needs to look for a "higher powered" solution.

Buster's technology is based many years experience managing networks, and on three ideas which we believe to be patentable. Being granted even one of these patents would present a significant barrier to potential competition. See Appendix A: Technology.

Buster units stay up to date with network problems by obtaining regular updates from our servers. Subscription fees from users or ISPs are expected to be the primary source of revenue. A subscription fee of $10 each month would be more economical for end users than anything currently on the market. When multiplied by 100 Million users, this represents a $1 billion per month market.

When implemented as a stand-alone device, COGS for a Buster is estimated at under $40 (See Appendix D: Financial Projections). The chipset version can be assembled from off-the-shelf chips of about $20. Designing customized chips could reduce these costs.

## Target Customers

Home and SOHO users are our initial customers. Most network management/security products target large corporate customers, since these companies have MIS staffs and budgets, and have the most to loose from a compromised network. This has left the fast growing home and SOHO market under-served.

Buster is a complete solution, is easy to deploy, cost competitive, and is the only solution that does not bog down the user's network and computer. Installing Buster is as simple as connecting it to the network and a power supply. The easy setup, net speed improvement, low cost, and one-stop solution make it a natural for the SOHO market.

Another reason for pursuing SOHO markets is the rapid growth. As the numbers of fortune 1000 computers on the Internet has stagnated, home and SOHO, and educational (K-12) usage continues to grow[2]. Additionally, the SOHO and home

[2] IDC: "Public sector computer sales soar in third quarter" Dec. 9, 2002.

users of all ages are rapidly becoming more network savvy, and each year better understand the costs and risks of viruses, spam, spyware, etc.

Buster has compelling features for the medium and large size corporate market too. However this market has an entrenched culture of using SNMP and high-end firewalls to secure their networks. Buster has the potential to retire a lot of expensive personnel and equipment, and as such may be met with some resistance. The most effective approach to this market may be to let Buster's SOHO success gradually sell by attraction rather than promotion.



**The Competitive Market**

Currently the SOHO market relies on a patchwork of un-integrated products. Windows software programs are used for virus checking, web-content blocking; ISP services are available for blocking spam and offensive Internet sites; and firewalls can protect against intrusion and denial of service (DOS) attacks. Appendix B: The Existing Market compares the best selling products in related product areas.

These existing products have shown that home and SOHO customers are willing to purchase software for prices from $30 to $60 and pay additional periodic fees for update services. Firewalls range from $69 SOHO NAT routers to high-end (six-figure) devices from Cisco and Checkpoint.

Interestingly, every single home market product is Windows Software, and thus offers no protection for non-windows machines, such as PDAs, security systems, or Internet controlled appliances. Buster technology could be expanded into these markets, as well.

**Distribution Channels**

A variety of channels are available for distributing Buster boxes, and thus laying the ground for a large subscriber base. Possibilities include:

- Partnerships with ISPs – We will aggressively partner with Internet Service Providers to distribute buster boxes. The advantages to ISPs are revenue from box and shared subscription sales, value added value to their service offerings, and a reduction of the bandwidth that is a major expense.
- Distribute boxes retail – Sales through Frys, Radio shack and other retailers. Sales performance incentive plans could be used to get Buster visible locations to encourage impulse buying.
- Cross licensing with existing anti-virus & net blocking players – We will license a popular virus database and Blocked Web site list. Part of the arrangement should be that the partners co-market Buster boxes.
- License buster chip sets to low-end Firewall vendors. Mass marketed SOHO firewalls from Netgear, Dlink, are always looking for features to distinguish

their products and add value. We should approach this market by integrating the Buster technology with Taiwanese providers such as Via and OleComm, that develop the underlying technologies used in these products.

- License buster chip sets to Network adapter vendors such as Intel, Realtec, and 3com. Ethernet adapters have become a low-cost commodity, and these vendors are in need of features which will allow them to charge a premium for their products.
- Direct sales, backed by SPAM advertising. Send out Bulk emails promising to end bulk email. Example subject: "If you got this SPAM, you don't have a buster".

**Financial Projections**

Buster should be on the market by the end of 2003 and account for 10% of the SOHO security market (100,000 units) by the end of 2004, 1 Million units in 2005, and 10 Million units in 2006.

Predicted costs and revenues for the years 2003 through 2006 are in the attached spreadsheets.

The company will need about **$1.5 Million** before becoming profitable in '04. By the end of 2006, net profit is projected to be **$1.7 Billion** on revenues of **$1.9 Billion**.

## Appendix A: Buster Technology

Buster differs from firewalls and PC software in that it can run anywhere on your network. Each buster device has a dedicated, self-configuring Ethernet port running in "promiscuous" mode. It can thus look at every packet on the network ("sniffing"), and decide if the packet (or the connection it represents) should be allowed.

### Detecting Problems

Buster examines every byte of every packet, looking for unwanted content such as virus code, links to add-banner and pop-up sites, or addresses of spyware programs. Buster's fast search algorithm (pending patent #3) allows it's low cost off-the-shelf CPU to compare the complete contents of every packet to tens of thousands of patterns that may indicate undesirable content (virus footprints, domain names). Importantly, it can perform this search at network speeds.

### Intercepting Unwanted Connections

Unwanted connections (Spyware, banner adds) can be either broken outright, or "highjacked", allowing the network manager to replace unwanted content with something else (pending patent #1). As an example, a parent who wants to block his children from a gaming web site could replace the site's homepage with reminder that students should be doing their homework. Banner ads could be replaced with pictures of your children or pets.

### Erasing Unwanted Packets

Unwanted packets which are not part of a connection (DOS attacks, security attacks) can be prevented by Buster's precise control of it's Ethernet device. When the buster receives the beginning of a disallowed packet, the Buster sends a signal on the Ethernet (pending patent #2). This causes a collision, effectively killing the unwanted packet. The Ethernet adapter on the receiving machine device does not even generate an interrupt, rendering DOS attacks harmless.

### SPAM Deletion

When a network user attempts to access an email server, Buster hijacks the user's connection. Buster then makes it's own connection to the server, and commences email downloading into a ram buffer. Email senders, subjects, and content headers are scanned for known spam. Non-spam email is then forwarded to the user. The spam is dropped.

## Scaling Capacity

Scaling capacity of the Buster design is essentially unlimited. Each of Buster's CPU intensive functions (firewall filtering, email buffering, etc.) may be performed by a separate buster box. Multiple boxes may be used to subdivide the labor of especially complex situations.

For example, firewalls have an upper limit to the size of their "rule set" – the number of IP addresses and port combinations they can monitor. If the set gets too big, the CPU cannot check every packet at net speed. Busters don't have this limitation. If a rule set becomes too large, another buster can be added and each one made responsible for a portion of the rule set. This is impossible with ordinary firewalls (or firewall software running on a PC) since a firewall must be inserted between the Internet and the machine(s) it's trying to protect. This means an overworked firewall can become a bottleneck for the entire network.

## Patents

The following technologies are all essential to the Buster technology, and all are potentially patentable. All are original ideas developed specifically for Buster, and searches of the US patent office database have produced no conflicting patents. Additionally, we're unaware of any "prior art" for the claims made in the patent applications.

1) Ethernet packet collisions controlled for security reasons.
2) TCP connection interception (spoofing) for performance reasons.
3) Fast pattern lookup

## Appendix B: The Existing Market

### Cost and Violability of Competing Solutions

This information is presented in two tables. The first lists examples of the best solutions that are currently available, along with their costs. The problems are numbered for reference in the second table.

| Problem | Example Solutions | Minimum Initial Cost | Performance Reduction |
|---|---|---|---|
| 1) Intrusion | Firewalls, custom software patches | $249 and up | Severe |
| 2) Site blocking | Surfcontrol, | $39 per user | Minor |
| 3) Viruses | Windows Anti-Virus software | $10 - $30 | Medium |
| 4) Email Spam | Windows software | $0 | Minor |
| " | ISP service | $0 | None |
| 5) Popup prevention | Windows Software | $0 | Minor |
| 6) Add blocking | Windows software, firewalls | $50 and up | None |
| 7) Add replacement | None | N/A | N/A |
| 8) DOS attacks | Firewalls, custom | $69 and up | Severe |
| " | Custom software patches | $0 | Severe |
| 9) Spyware blocking | Windows Software | $0 | Minor |
| 10) Email security | Windows Software | $39 per user | Minor |

The second table lists some of the most popular commercial solutions by name, along with costs, benefits, and drawbacks. Pricing infomation is priced based on Google searches.

| **Class**/Product | Problems Addressed | Initial Cost | Maintenance | Notes |
|---|---|---|---|---|
| **Traditional Firewalls** | | | | |
| Checkpoint Firewall-1 Small Office (5 IPs) | 1,2,8 | $247.81 | $493/yr. [5] | [1],[2],[4] |
| Cisco PIX – 10 Users | 1,2,8 | $460 | $50/yr | [2],[3], |
| **Site Blocking Software** | | | | |

| | | | | |
|---|---|---|---|---|
| Websense (2) 50 users | 2,9 | Subscription only | $1196/yr. | [4],[6] |
| Surfcontrol (2) 50 users | 2 | Subscription only | $1180/yr | [4],[6] |
| Cybersitter 1 user | 2 | $39 | ???[7] | [4],[6],[8] |
| **Single PC Firewalls** | | | | |
| Zone Labs Zone Alarm Pro 3.5 | 1,5,6,9 | $49.95 | $69.90/2 years | [4],[6] ,[8] |
| Norton Internet Security 2003 | 2,3,4,5,6,8 | $69.95 | $39.95 [9] | [4],[6] ,[8] |
| McAfee Internet security 5.0 | 1,2,3,5,8 | $70 | ??? no info | [4],[6] ,[8] |

Notes:
[1] Only handles 5 IP addresses
[2] Includes VPN function
[3] Hardware product
[4] Software product
[5] 100 IP addresses - lowest price available
[6] Degrades Windows system performance
[7] They claim "no recurring fees", however they also offer "premium subscription service" for $20 for 2 years.
[8] Only protects one windows machine
[9] Upgrade from last years version

Sources:
(1) Market leader according to Gartner Group
(2) Market leaders per Infonetics

## Appendix C: Management

**John Bartas**
**408-257-3414**
**jbartas@iniche.com**



Founder and technical lead of Interniche Technologies, the leading supplier of Internet technology for embedded devices. Over twenty years networking experience on all types of systems. Pioneered technologies bringing the Internet to Microcomputers starting in 1985. Contributed to Internet standards and developed ideas still in use in most current networked devices.

**Employment:**

**1996 – Present** **CTO, Interniche Technologies**

In 1996 launched Interniche with a Web-managed NAT routing product. Managed a technical staff that grew to eight engineers. Personally wrote an embedded Web browser which fits in 35K of code space, and obtained a U.S. patent for the HTML parsing design which enables it's small size. Interniche products consistently win technical "bake-offs", and we have put every competitor we had out of business.

Guest speaker at Intel presentation, Interop2000 Conference in Las Vegas; and also EIC conference in 2001 in San Jose. Taught intensive TCP/IP engineering seminars in Europe and United States. Currently producing a dual IPv4/IPv6 stack for embedded devices.

**1988 – 1995** **Startup Experience**

Software Engineering for network startups, often as a consultant; specializing in prototyping early products for company equity. Successes include Kalpana, Cybermedia, Network General and NetFrame. Only one company (out of seven) in which I worked for stock options or warrants did not eventually IPO or get acquired.

**1985 - 1988** **The Wollongong Group**

Implemented the first commercially successful TCP/IP stack for IBM PCs. Developed the first dynamically unloadable network device driver, a concept used in virtually all networked PCs today; and developed the first PC-based IP router. Led a team that implemented the first IP tunneling product and resulted in the first IP tunneling standard, RFC-1088.

**1984** **Octel Communications**

Wrote device drivers and test software for the Octel Communications "Aspen", a pioneering voice messaging system.

**1981 – 1983** **Rothenberg Information Systems**

Repaired Microcomputer hardware and did systems programming in C and assembly on the CP/M operating system. Prototyped a Z80 based print server. Wrote medical billing and insurance applications in BASIC language for Rothenberg customers.

## Education

1983 – DeAnza College. Courses in Computer science and Business.
1978 – BA -University of Connecticut. Art major, minor in molecular biology

## Other Activities

- Listed as contributor in 2 Internet standard documents. RFC-1088 and RFC-2775
- Member of the IETF NAT routing working group.
- Member of the IETF IPv6 working group.
- Second US Patent (pending) for IP address expansion technique
- Book Contract with CMP publishing for "Embedded PPP - The PPP protocol in embedded systems", Due to be published by CMP in 2003.

## Appendix D: Financial Projections

**Projected Revenue, 2003 – 2006**

| | Year: | 2003 | 2004 | 2005 | 2006 |
|---|---|---|---|---|---|
| Revenue | | | | | |
| | Subscribers (count) | 100 | 100,000 | 1,100,000 | 11,100,000 |
| | Sales (@$10.mo) | $1,2000 | $12,000,000 | $131,000,000 | $1,332,000,000 |
| | Licensing Rev. | 100,000 | 100,000 | 100,000 | 100,000 |
| | Number of OEMS | 3 | 5 | 7 | 9 |
| | Est. cash income | 300,000 | 500,000 | 700,000 | 900,000 |
| | Units sold | 100 | 100,000 | 1,000,000 | 10,000,000 |
| | Unit sales @ $60/ea. | 6000 | 6,000,000 | 60,000,000 | 600,000,000 |
| | Total Revenue | 418,103 | 18,700,005 | 192,800,007 | 1,943,000,009 |
| Costs | (See other sheet) | 1,550,010 | 4,390,018 | 24,780,033 | 215,610,049 |
| **Net Profit** | | **($1,131,907)** | **$14,309,987** | **$168,019,974** | **$1,727,389,960** |

- (Costs on next page) -

**Projected Costs, 2003 – 2006**

| Year: | 2003 | 2004 | 2005 | 2006 |
|---|---|---|---|---|
| Costs | | | | |
| Salaries | | | | |
| Officers | 2 | 2 | 2 | 3 |
| - Expense | $300,000 | $300,000 | $400,000 | $600,000 |
| Sales/marketing staff | 2 | 4 | 8 | 16 |
| - Expense | 300,000 | 550,000 | 800,000 | 1,600,000 |
| Engineering staff | 4 | 5 | 9 | 12 |
| - Expense | 440,000 | 550,000 | 1,000,000 | 1,400,000 |
| Content research | 2 | 4 | 8 | 10 |
| - Expense | 200,000 | 400,000 | 800,000 | 1,000,000 |
| Manfucturing | 1 | 3 | 5 | 6 |
| - Expense | 100,000 | 220,000 | 400,000 | 460,000 |
| Other | 1 | 2 | 3 | 5 |
| - Expense | 60,000 | 130,000 | 200,000 | 350,000 |
| COGs | | | | |
| Units | 100 (prototype) | 100,000 | 1,000,000 | 10,000,000 |
| Expense | 50,000 | 2,000,000 | 20,000,000 | 200,000,000 |
| Rent | 50,000 | 70,000 | 90,000 | 100,000 |
| Other | 50,000 | 70,000 | 90,000 | 100,000 |
| Total Expense: | $1,550,010 | $4,390,018 | $24,780,033 | $215,610,049 |

COPY

# Stat ment of Invention and Intent to Patent.

John Bartas
1/2/2003

I, John Bartas, declare that the idea(s) described in this document, are my own, that I believe them to have commercial value, and that I intend to file a United States Patent application. When notarized, this document will serve as proof of a date by which the idea had been developed.

## Invention:

This invention is a software algorithm to rapidly search a stream of data for a large number (many thousands) of patterns (herein "the patterns") which may appear in the data stream. It will be useful for searching networked packets for virus signatures and other content that warrants attention.

The algorithm is based on hashing. Since it is not known where (or even if) any of the patterns appear in the data, we must search the data stream for a match to every pattern, starting at every byte in the data stream. To accelerate this, we choose a length of data to hash – perhaps on the order of 10 bytes (the "sum field). Our first hash value is derived for the first 10 bytes of the data, using a summing algorithm that has this characteristic: Subtracting any byte from the sum will restore the value that would be in the sum if the byte had not been added.

Once the sum for bytes 1-10 has been obtained, it is used to index a large table containing pre-hashed values for all the patterns. This table should be large enough so that most hash buckets are empty, allowing the lookup to return a fast "no match" most of the time.

The next step is to obtain the hash sum for bytes 2-11. This is done by adding the next byte (the 11th) to the sum, and subtracting the first byte. This yields the value of bytes 2-11 without recomputing the whole sum. This is repeated for bytes 3-12, 4-13, etc; moving the sum field through to the end of the data stream.

Note that it may be advantageous to sum 16-bit (or larger) fields rather than bytes, using ones complement addition, and wrapping the carry bit. In the 16 bit case two sums will be maintained, one for words on odd byte boundaries and one for even byte boundaries..

John Bartas

Please see a one page CA ACK FORM attached to this document.
B. Ramakabir NOTARY PUBLIC.

B. D. RAMAKABIR
Commission # 1295465
Notary Public - California
Santa Clara County
My Comm. Expires Feb 26, 2005

COPY

## CALIFORNIA ALL-PURPOSE ACKNOWLEDGMENT

State of California

County of SANTA CLARA } ss.

On JAN 3, 2003 (Date), before me, B D RAMAKABIR ( NOTARY PUBLIC ) (Name and Title of Officer (e.g., "Jane Doe, Notary Public"))

personally appeared JOHN BARTAS (Name(s) of Signer(s))

☐ personally known to me
☒ proved to me on the basis of satisfactory evidence

to be the person(~~s~~) whose name(~~s~~) is/~~are~~ subscribed to the within instrument and acknowledged to me that ~~he~~/she/~~they~~ executed the same in his/~~her/their~~ authorized capacity(~~ies~~), and that by his/~~her/their~~ signature(~~s~~) on the instrument the person(~~s~~), or the entity upon behalf of which the person(~~s~~) acted, executed the instrument.

B. D. RAMAKABIR
Commission # 1295465
Notary Public - California
Santa Clara County
My Comm. Expires Feb 26, 2005

WITNESS my hand and official seal.

B D Ramakabir
Signature of Notary Public

Place Notary Seal Above

### OPTIONAL

*Though the information below is not required by law, it may prove valuable to persons relying on the document and could prevent fraudulent removal and reattachment of this form to another document.*

**Description of Attached Document**

Title or Type of Document: HASHING ALGORITHM

Document Date: JAN 2, 2003 Number of Pages: ONE

Signer(s) Other Than Named Above: NONE

**Capacity(ies) Claimed by Signer**

Signer's Name: _____

☐ Individual
☐ Corporate Officer — Title(s): _____
☐ Partner — ☐ Limited ☐ General
☐ Attorney in Fact
☐ Trustee
☐ Guardian or Conservator
☐ Other: _____

Signer Is Representing: _____

RIGHT THUMBPRINT OF SIGNER
Top of thumb here

COPY

# Statem nt of Invention and Intent to Patent

John Bartas
1/2/2003

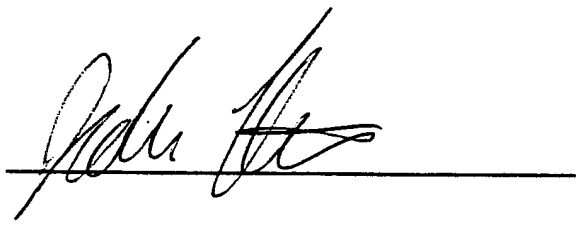
I, John Bartas, declare that the idea(s) described in this document, are my own, that I believe them to have commercial value, and that I intend to file a United States Patent application. When notarized, this document will serve as proof of a date by which the idea had been developed.

## Invention:

The idea is the use Ethernet hardware to deliberately generate collisions or other disruptive conditions an Ethernet in order to control the content of a network. The disruption will cause the Ethernet nodes on the network to discard the disrupted frame. The idea may apply to other network, such as wireless LANs.

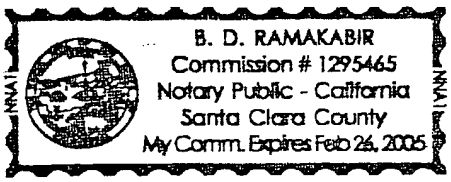
Advantages include lessening processing burdens on the CPUs attached the Ethernet nodes, and protecting them from malicious content in the frames; such as DOS attacks and Spyware.

John Bartas



Please see a one page CA ACK FORM attached to this document.

B. Ramakabir
NOTARY PUBLIC.



# CALIFORNIA ALL-PURPOSE ACKNOWLEDGMENT

State of California

County of SANTA CLARA } ss.

On JAN 3, 2003 (Date), before me, B D RAMAKABIR ( NOTARY PUBLIC ) (Name and Title of Officer (e.g., "Jane Doe, Notary Public"))

personally appeared JOHN BARTAS (Name(s) of Signer(s))

☐ personally known to me

☒ proved to me on the basis of satisfactory evidence

to be the person(s) whose name(s) ~~is/are~~ subscribed to the within instrument and acknowledged to me that ~~he/she/they~~ executed the same in ~~his/her/their~~ authorized capacity~~(ies)~~, and that by ~~his/her/their~~ signature~~(s)~~ on the instrument the person~~(s)~~, or the entity upon behalf of which the person~~(s)~~ acted, executed the instrument.

B. D. RAMAKABIR
Commission # 1295465
Notary Public - California
Santa Clara County
My Comm. Expires Feb 26, 2005

WITNESS my hand and official seal.

B Ramakabir
Signature of Notary Public

Place Notary Seal Above

## OPTIONAL

*Though the information below is not required by law, it may prove valuable to persons relying on the document and could prevent fraudulent removal and reattachment of this form to another document.*

**Description of Attached Document**

Title or Type of Document: ETHERNET COLLISIONS

Document Date: JAN 2, 2003 Number of Pages: ONE

Signer(s) Other Than Named Above: NONE

**Capacity(ies) Claimed by Signer**

Signer's Name: _____

☐ Individual
☐ Corporate Officer — Title(s): _____
☐ Partner — ☐ Limited ☐ General
☐ Attorney in Fact
☐ Trustee
☐ Guardian or Conservator
☐ Other: _____

Signer Is Representing: _____

RIGHT THUMBPRINT OF SIGNER
Top of thumb here

COPY

# Statement of Inv ntion and Intent to Patent.

John Bartas
1/2/2003

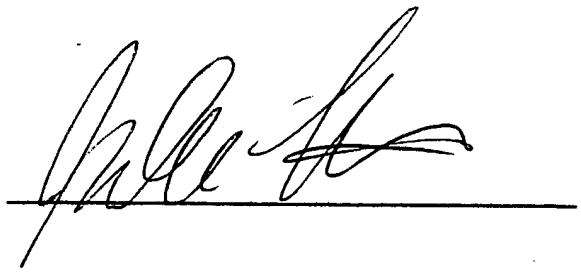
I, John Bartas, declare that the idea(s) described in this document, are my own, that I believe them to have commercial value, and that I intend to file a United States Patent application. When notarized, this document will serve as proof of a date by which the idea had been developed.

## Invention:

The invention is using "IP/TCP spoofing" to monitor and possibly edit content of a TCP connection. Spoofing consists of having one machine falsely assume the IP address of another in order to intercept traffic bound the other machine. It is used without the consent or knowledge of the parties to the transaction, usually for nefarious purposes.

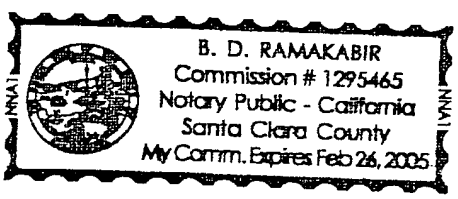
The original idea herein is to use spoofing with the consent of the network's owner in order to remove unwanted content. This can include viruses, Spam, and contents of advertising images and text. This content can either be removed, or replaced with other content. This idea also covers resetting TCP/IP connections to ease the effect of DOS attacks (e.g. SYN floods), and thwarting security probes of TCP ports by returning false information to the probe.

John Bartas



Please see a one page CA ACK FORM attached to this document.

B Ramakabir
NOTARY PUBLIC.



COPY

# CALIFORNIA ALL-PURPOSE ACKNOWLEDGMENT

State of California
County of SANTA CLARA } ss.

On JAN 3, 2003 (Date), before me, B D RAMAKABIR ( NOTARY PUBLIC ) (Name and Title of Officer (e.g., "Jane Doe, Notary Public")),
personally appeared JOHN BARTAS — (Name(s) of Signer(s)),

☐ personally known to me
☒ proved to me on the basis of satisfactory evidence

to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they executed the same in his/her/their authorized capacity(ies), and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

WITNESS my hand and official seal.

B. D. RAMAKABIR
Commission # 1295465
Notary Public - California
Santa Clara County
My Comm. Expires Feb 26, 2005

Place Notary Seal Above

Signature of Notary Public

## OPTIONAL

*Though the information below is not required by law, it may prove valuable to persons relying on the document and could prevent fraudulent removal and reattachment of this form to another document.*

**Description of Attached Document**
Title or Type of Document: IP/TCP SPOOFING
Document Date: JAN 2, 2003 Number of Pages: ONE
Signer(s) Other Than Named Above: NONE

**Capacity(ies) Claimed by Signer**
Signer's Name:
☐ Individual
☐ Corporate Officer — Title(s):
☐ Partner — ☐ Limited ☐ General
☐ Attorney in Fact
☐ Trustee
☐ Guardian or Conservator
☐ Other:
Signer Is Representing:

RIGHT THUMBPRINT OF SIGNER
Top of thumb here